Key Conversion Method For Communication Session Encryption And Authentication System

ABSTRACT

An interactive mutual authentication protocol, which does not allow shared secrets to pass through untrusted communication media, integrates an encryption key management system into the authentication protocol. The server encrypts a particular data random key by first veiling the particular data random key using a first conversion array seeded by a shared secret, and then encrypting the veiled particular data random key. The client decrypts and unveils the particular data random key using the shared secret, and returns a similarly veiled version of the particular data random key using a second conversion array seeded by a shared secret. Access to the shared secret indicates authenticity of the stations. The procedure may be repeated for a second shared secret for strong authentication, without allowing shared secrets to pass via untrusted media.